Remarks and Arguments

Claims 1-128 have been presented for examination. Claims 2, 5, 13, 16, 24, 27, 35, 38, 59, 66, 101 and 108 have been amended. Claims 1, 8-12, 19-23, 30-34, 41-58, 73-100 and 115-128 have been canceled. Claims 129-140 have been added.

Claims 1-128 have been rejected under 35 U.S.C. §103(a) as obvious over U.S. Patent No. 5,220,604 (Gasser, previously cited) in view of U.S. Patent No. 5,339,403 (Parker, previously cited.) The examiner comments that the Gasser reference discloses credentials that include nested groups with chains of group credentials, but, in Gasser, the credentials must be looked up for comparison and Gasser does not disclose making the credentials available to the group. However, the examiner asserts that the Parker reference discloses the presentation of credentials that contain user access rights and are organized by grouping. The examiner concludes that it would have been obvious to one skilled in the art to combine the teachings of Gasser and Parker because Parker discloses that a user needs to be authenticated once and the resulting privilege attribute certificate can be reused to access several different applications and thus it would have been obvious to combine the references in order to speed up the process of accessing multiple applications as disclosed by Parker.

The present invention relates to a method and apparatus for controlling access to a resource based on membership or non-membership in a group that is a sub-group of a nested group. In particular, when a client requests access to a resource that is controlled by a resource server, if the client does not itself have sufficient credentials to permit such access, the resource server returns a "challenge", or request, for additional credentials, specifically credentials proving membership or non-membership in a group, as set forth in the instant specification at page 8, lines 9-23. In response to this challenge, the client itself performs a search to locate the group credentials. In the inventive system, each group is controlled by a group server and the client may make a request to a group server for credentials indicating membership or non-membership in the group controlled by that server. This latter request may include credentials indicating membership or non-membership in a sub-group which allow the group server to make a determination of membership or non-membership. Thus, in the inventive system both the server which controls the resource and the client which requests access to the

resource perform searches in order to make a decision whether access should be granted.

As previously discussed, the Gasser reference discloses an access control system in which a resource server that controls resources performs a search over groups to determine whether access will be granted to a client that is a member of that group. The client does not participate in this search. This operation is described at several places in the Gasser reference. See, for example, Gasser, column 3, lines 24-28 and lines 55-63 and column 5, lines 29-34 (where a reference monitor controlling the resource determines whether access will be granted by checking an access control list or verifying membership in a group.) Similarly, Gasser discloses authentication procedure between two principals P1 and P2 at column 6, line 48-column 7, line 37 and at column 9, lines 16-48. Here it is clear that the client (the principal requesting authentication (P1)) merely presents a nonce encrypted with a private key to principal P2 and principal P2 does the rest of the work including any lookups required.

Thus, as the examiner notes, Gasser does not teach or suggest that the client should participate in search required the access granting or authentication process and then present the results of the search to the server for authentication.

The examiner proposes to combine the Parker reference with Gasser in order to provide a teaching that the client should provide access control or authentication information to the resource. As previously stated, in Parker, the information that the client provides to the resource consists of access rights that have already been determined. Parker does not disclose that the client perform a search to get authentication information that will later be used by the server to determine the access rights to the resource. More specifically, Parker does not disclose the client performing a search to prove membership in a group.

Thus, neither reference discloses that the client should perform a search to locate additional credentials for proving membership or non-membership in a nested group. In order to particularly point out these differences, the independent claims have been canceled and reworded. For example, claim 1 has been canceled and reworded as new claim 129. Claim 129 recites, in lines 8-13, "... in response to the challenge (from the server), performing a search at the client to obtain a chain of group credentials

that proves membership in the nested group, and presenting from the client to the resource server a second request to access the resource, the second request including the chain of group credentials." As discussed previously, neither reference discloses or suggests using the client to perform part of the credential search. Thus, claim 129 patentably distinguishes over the cited combination of references.

New claims 130 and 131 have been added to further point out aspects of the search performed by the client. New claim 130 recites that membership in each group is controlled by a group server and the client contacts at least one group server to obtain group credentials for the group controlled by that server. New claim 131 recites that the client may present to the group server credentials that prove membership in a sub-group nested within the group controlled by the server to prove membership. These features are described in the instant specification at page 8, line 24 to page 9, line 23. Neither Gasser nor Parker discloses a client requesting group credentials from group servers that maintain credentials for a group. Thus, new claims 130 and 131 also patentably distinguish over the cited reference combination.

Claims 2-7 have been amended to be dependent, either directly or indirectly, on claim 129 and, thus, incorporate the limitations thereof. Therefore, they distinguish over the cited reference combination in the same manner as claim 129. Claims 8-11 have been canceled thereby rendering the rejection thereof moot.

Claim 12 has been canceled and rewritten as new claim 132. New claim 132 recites limitations that parallel those recited in claim 129 with the exception that the credentials obtained and presented by the client prove client non-membership in a group. Claim 132 patentably distinguishes over the cited reference combination in the same manner as claim 129 as discussed above. New claims 133 and 134 contain limitations that parallel those in claims 130 and 131 and distinguish over the cited reference combination in the same manner as claims 130 and 131.

Claims 13-18 have been amended to be dependent, either directly or indirectly, on claim 132 and, thus, incorporate the limitations thereof. Therefore, they distinguish over the cited reference combination in the same manner as claim 132. Claims 19-22 have been canceled, thereby rendering the rejection thereof moot.

Claims 23 and 31 have been canceled and rewritten as new claims 135 and 138. New claims 135 and 138 recite limitations that parallel those recited in claims 129 and 131, respectively. Therefore, claims 135 and 138 patentably distinguish over the cited reference combination in the same manner as claims 129 and 131, as discussed above. New claims 136-137 and 139-140 contain limitations that parallel those in claims 130 and 131 and distinguish over the cited reference combination in the same manner as claims 130 and 131.

Claims 24-30 and 35-40 have been amended to make them dependent, either directly or indirectly, on claims 135 and 138, respectively, and incorporate the limitations thereof. Therefore, they distinguish over the cited reference combination in the same manner as claims 135 and 138. Claims 41-58 have been canceled thereby rendering the rejections thereof moot.

Claims 59, 101 and 66, 108 have been amended to recite limitations that parallel those recited in claims 129 and 131, respectively. Thus, claims 59, 66, 101 and 108 patentably distinguish over the cited reference combination in the same manner as claims 129 and 131 as discussed above.

Claims 60-65, 102-107 and 67-72, 109-114 are dependent, either directly or indirectly, on claims 59, 101 and 66, 108, respectively, and incorporate the limitations thereof. Therefore, they distinguish over the cited reference combination in the same manner as claims 59, 66, 101 and 108. Claims 73-100 and 115-128 have been canceled thereby rendering the rejection thereof moot.

In light of the forgoing amendments and remarks, this application is now believed in condition for allowance and a notice of allowance is earnestly solicited. If the examiner has any further questions regarding this amendment, he is invited to call

applicants' attorney at the number listed below. The examiner is hereby authorized to charge any fees or direct any payment under 37 C.F.R. §§1.17, 1.16 to Deposit Account number 02-3038.

Respectfully submitted

Paul E. Kudirka Date: 2/28/06

Paul E. Kudirka, Esq. Reg. No. 26,931
KUDIRKA & JOBSE, LLP
Customer Number 045774
Tel: (617) 367-4600 Fax: (617) 367-4656